IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW MEXICO

IN RE SEARCH WARRANT
APPLICATION FOR LOCATION
INFORMATION.

Case No. 1:24-mr-01454-SCY

MEMORANDUM OPINION AND ORDER
DENYING WARRANT APPLICATION

The ability to track the suspect of a crime has long been vital to many successful law enforcement investigations. Before cell phones, beepers, and radio transmissions, law enforcement tracked suspects through discreet first-hand visual surveillance. Now that most Americans carry a cell phone on their person almost anywhere they go, law enforcement frequently tracks suspects of crimes through signals emitted from their cell phones. In what are commonly referred to as "ping warrants," law enforcement obtains an order from a court that requires cell phone companies to disclose, at all times day or night and typically for a period of thirty days, all location information emitted from a suspect's cell phone. Many of these orders also require the cell phone company to initiate a signal at the request of law enforcement at regular intervals during this tracking period.

That law enforcement has the ability to obtain a search warrant to track a person's location is not in dispute. Exactly what authority allows a court to order a cell phone company to initiate signals or to provide prospective records of a customer's location on a rolling basis for an extended time, however, has been the subject of considerable debate. The United States argues, and agents represent in their affidavits, that such authority derives from a portion of the Stored Communications Act ("SCA"), 18 U.S.C. § 2703, as well as Rule 41 of the Federal Rules of Criminal Procedure. The United States Supreme Court has recognized that the government can

obtain historical cell site location information—that is, a record of past movement—through a § 2703 search warrant. *Carpenter v. United States*, 585 U.S. 296, 316-17 (2018). But the SCA is silent as to rolling, prospective information shared at all times day or night over an extended period. Thus, to satisfy courts that have questioned whether the SCA and Rule 41 provide authority for agents to obtain location information on a rolling basis over an extended period, the government also requests a Pen Register and Trap and Trace ("PRTT") order pursuant to 18 U.S.C. §§ 3122 and 3123 (the "Pen/Trap Statute") at the same time it submits its warrant request.[1]

In considering the United States' ping warrant application, the Court first addresses whether the SCA on its own authorizes the collection of prospective location information on a rolling basis. Second, the Court addresses whether the SCA can combine with the Pen/Trap Statute to provide such authority. Third, the Court addresses whether the cell phone being tracked should be considered a tracking device. This last question matters to law enforcement because jurisdictional provisions contained in the Tracking Device Statute ("TDS"), 18 U.S.C. § 3117, are narrower than jurisdictional provisions in the SCA, 18 U.S.C. § 2711, and because Rule 41 contains specific procedural requirements that apply to tracking devices that the United States argues do not apply to ping warrants.

[1] The United States does not seek an order under the All Writs Act, 28 U.S.C. § 1651. Further, unrelated to the ping order request, the United States also applied for a "Stingray" warrant—permission to use what is essentially a portable device that mimics a cell phone tower. Law enforcement sought to use this device to collect the suspect's cell phone signals and to determine the location of that cell phone. The Court initially denied the United States' application. After the September 6, 2024, hearing, the United States submitted a third application for use of this "Stingray" warrant which the Court granted. As a result, the United States' submission of an application for use of a "Stingray" device is not addressed in this Order.

For the reasons below, the Court denies the United States' ping warrant application. It finds that 1) the SCA does not, on its own, permit the government to obtain prospective location information, but that 2) the SCA in combination with the Pen/Trap Statute does permit such prospective information. This combination 3) renders the cell phone a tracking device subject to the TDS and procedural requirements for tracking devices under Rule 41. Having so concluded, the Court also sets forth procedures the United States must follow when submitting future warrants to the undersigned that seek extended rolling real-time disclosure of location information emitted from a suspect's cell phone.

BACKGROUND

For at least the last ten years, the United States has been submitting requests for ping warrants in a format substantially similar to the ping warrant currently at issue. Part of the United States' stock language has included a request to order a cell phone company to create location records by initiating a signal ("pinging" the suspect's cell phone) so that law enforcement could then seize the record. And for the past ten years, the undersigned has been rejecting this request by either having the United States resubmit applications that do not contain this language or by crossing this language out from the search warrant attachments it authorizes. On July 19, 2024, the United States sought to obtain a target's location information by sending signals to an internal modem located inside a target's vehicle. Case No. 1:24-mr-01391-SCY, Doc. 1 at 1.[2] The application did not indicate that the provider already initiated such signals in the ordinary course of its business. The Court found that compelling a third party to create records it would not have otherwise created so that law enforcement could then seize those records went beyond the scope

[2] Citations to the record in this paragraph and the following paragraph refer to the record in Case No. 1:24-mr-01391-SCY.

of Federal Rule of Criminal Procedure 41 and 18 U.S.C. § 2703(c)(1)(A), the authority on which the United States based its request. *Id.* at 1-2. Accordingly, the Court denied the warrant application. *Id.* at 2. On July 24, 2024, the United States resubmitted the search warrant without removing the "initiating a signal" language the Court had just rejected. *Id.* at 2-3. The Court thus set a hearing to address the issue, at which an attorney from the Federal Public Defender's Office ("FPD") also appeared upon the Court's invitation. *Id.* at 3-4.

At the hearing on August 1, 2024, the government and the FPD presented arguments on the issue. *See generally* Doc. 5. The United States represented that no case or controversy existed; the "initiate a signal" language was a clerical error, *id.* at 12:22-24, and the United States did not intend to use that language in future warrant applications for prospective location information, *id.* at 12:7-13. The Court accepted the United States' representation that the language was erroneous, and as such, closed the matter as moot on August 3, 2024. Doc. 4.

On August 5, 2024, the United States submitted a warrant application in an unrelated case—the case at issue presently, No. 1:24-mr-01454-SCY. Doc. 1 at 1.[3] This application sought to obtain a target's cell phone location information and once again included the "initiate a signal" language that, the week before, the United States represented was submitted in error and that it no longer intended to use. *Id.* at 2-3. Because the resubmission of this "initiate a signal" language indicated the issue actually was not moot, and because the Court also had concerns about whether Rule 41 procedures related to tracking devices should be followed, the Court ordered the

[3] This citation and all citations to the record hereafter refer to the case for which this memorandum opinion and order is written: No. 1:24-mr-01454-SCY.

United States to file a brief addressing the relevant issues and set the matter for a hearing.[4] *Id.* at 3. The Court also invited, but did not require, the FPD to attend the hearing and submit a brief. *Id.* The United States sought a continuance and extension of the briefing deadline to August 20, 2024. Doc. 3. The Court granted this motion. Doc. 4. On August 15, 2024, the United States resubmitted its warrant application. This resubmission, among other things, removed the "initiating a signal" language to which the Court objected. The United States timely submitted its brief, Doc. 5, the FPD filed no response, and the Court held a hearing on September 6, 2024. Doc. 6.

At the September 6, 2024, hearing, consistent with its brief, the United States argued: 1) § 2703 of the SCA allows for disclosure of prospective location information on its own, Doc. 5 at 3-5; 2) a warrant for prospective location information from a cell phone does not make that cell phone a tracking device subject to the TDS, *id.* at 6-9; 3) because a cell phone is not a tracking device and a warrant for prospective location information is not a tracking warrant, the tracking warrant procedures in Rule 41 do not apply, *id.* at 9-10; and 4) although § 2703 is sufficient on its own to obtain prospective location information, it can also work in conjunction with the Pen/Trap Statute as supported by certain language in the 1994 Communication Assistance for Law Enforcement Act ("CALEA"), 47 U.S.C. § 1002(a)(2), *id.* at 11-12.

The United States also argued at the September 6 hearing that the location information cell phone companies provide law enforcement is not precise, which prompted the Court to point

[4] These issues included 1) whether a ping warrant functioned as a tracking device such that the tracking device provisions in Rule 41 applied, 2) whether Rule 41 or the SCA allow the Court to order a provider to produce prospective information, 3) whether the PRTT statute applies, 4) whether the PRTT statute allows the United States to obtain the prospective location information requested, and 5) whether the above issues will be moot if the United States withdraws this warrant and submits a revised warrant. *Id.* at 3.

out that its warrant application requests E-911 Phase II data. The requesting agent's affidavit notes that E-911 Phase II data is "also known as GPS data or latitude-longitude data" and that "E-911 Phase II data provides relatively precise location information about the cellular telephone itself, either via GPS tracking technology built into the phone or by triangulating on the device's signal using data from several of the provider's cell towers." Doc. 8 at 10 ¶ 27 (Ping AO106a). This data, according to the affidavit, is different than "cell-site data" which "identifies the 'cell towers' (i.e., antenna towers covering specific geographic areas) that received a radio signal from the cellular telephone and, in some cases, the 'sector' (i.e., faces of the towers) to which the telephone connected." *Id.* at 10-11, ¶ 27. Accordingly, the affidavit continues, "cell-site data is typically less precise that [sic] E-911 Phase II data." *Id.* at 11 ¶ 27. This cell site data is often referred to as cell site location information, or "CSLI". *See, e.g.*, *Carpenter*, 585 U.S. at 300-01.

In response to the Court's observation that the United States is seeking an order for a suspect's precise location (through E-911 Phase II data) for the next thirty days, the United States offered to withdraw its requests for E-911 Phase II data so that the Court would only be ordering the cell phone company to provide CSLI. Doing so, however, would not change the Court's analysis. Although E-911 Phase II data may provide more precise location information than CSLI, the Court concludes that, even when the government tracks a person's movements at all times day or night for thirty days through the less precise CSLI, the degree of invasion into that person's reasonable expectation of privacy is sufficiently high that it cannot be justified without a warrant.[5] This conclusion is consistent with *Carpenter*, which only involved CSLI. 585 U.S. at 300-01.

[5] Unlike in *Carpenter*, the United States here seeks a warrant for the location information it desires. Thus, whether the suspect in the present matter has a reasonable expectation of privacy

The Supreme Court described the United States' argument in *Carpenter* as follows: "[T]he collection of CSLI should be permitted [without a warrant] because the data is less precise than GPS information. Not to worry, they maintain, because the location records did 'not on their own suffice to place [Carpenter] at the crime scene'; they placed him within a wedge-shaped sector ranging from one-eighth to four square miles." *Id*. at 312. The Supreme Court rejected the United States' argument that the distinction between CSLI and more precise GPS location data compels a different result regarding the necessity of a warrant:

> [T]he rule the Court adopts must take account of more sophisticated systems that are already in use or in development. While the records in this case reflect the state of technology at the start of the decade, the accuracy of CSLI is rapidly approaching GPS-level precision. As the number of cell sites has proliferated, the geographic area covered by each cell sector has shrunk, particularly in urban areas. In addition, with new technology measuring the time and angle of signals hitting their towers, wireless carriers already have the capability to pinpoint a phone's location within 50 meters. Accordingly, when the Government accessed CSLI from the wireless carriers, it invaded Carpenter's reasonable expectation of privacy in the whole of his physical movements.

Id. at 313 (internal quotations and citations omitted). Similar to the Supreme Court's decision in *Carpenter* that the distinction between GPS location data and CSLI did not compel a different result regarding the necessity of a warrant, the Court here concludes this distinction does not compel a different result for any of the issues presently before it. Because this distinction does not impact the Court's analysis and because the United States argued that it was willing to

---

in the records the United States seeks is irrelevant. Nonetheless, because a primary focus of the United States' presentation at the September 6 hearing involved the type of location information sought, the Court addresses the significance, or lack of significance, of the difference between GPS location information and CSLI.

withdraw its request for E-911 Phase II data, the Court hereinafter refers to the location data the United States seeks as CSLI.[6]

LEGAL STANDARD

Before addressing the substance of the United States' arguments, the Court pauses to provide a brief summary of the relevant statutes.

The Electronic Communications Privacy Act of 1986 ("ECPA") broadly governs several types of electronic communications. Title I regulates wiretaps (shorthand for real-time interception of the contents of wire, oral, or electronic communications, *see* 18 U.S.C. § 2510) by requiring extensive criteria be met before obtaining a court-authorized wiretap. *See* 18 U.S.C. § 2518. Title III regulates pen registers and trap and trace devices, which record outgoing and incoming phone information. 18 U.S.C. § 3127. Specifically, PRTT devices record the dialing, routing, addressing, and signaling information—essentially, the phone numbers with which the subject cell phone has communicated—but not the contents of those communications, which remain governed by Title I's wiretap provisions. *Id.* In another short section, ECPA contains the Tracking Device Statute, 18 U.S.C. § 3117, which defines a tracking device and provides jurisdictional rules. (Tracking devices are also governed by Rule 41 of the Federal Rules of Criminal Procedure, which addresses how to obtain a warrant for a tracking device and the limitations attendant to such warrants.) All of these forms of prospective real-time monitoring—contents of communications, dialing information, and location tracking—can only take place for a limited period. *See* 18 U.S.C. § 2518(5); 18 U.S.C. § 3123(c); Fed. R. Crim. P. 41(e)(2)(C).

[6] The Court notes that, although the United States offered to resubmit a search warrant application that did not include a request for E-911 Phase II data, the Court did not ask it to do so and the United States never did so. Such a resubmission would serve no purpose, as the difference between E-911 Phase II data and CSLI has no bearing on the Court's present analysis.

Additionally, they all require some form of disclosure after the interception is complete, whether a report of the number of wiretap or PRTT orders granted each year, 18 U.S.C. § 2519, 18 U.S.C. § 3126, or service of the warrant on the person tracked, Fed. R. Crim. P. 41(f)(2)(C).

Title II of the ECPA is frequently referred to as the Stored Communications Act,[7] 18 U.S.C. §§ 2701-13, and it differs from the other portions of the ECPA. Unlike the provisions previously discussed, the SCA is not limited to a specific type of information. Rather, it is more general, allowing the Court to order a phone service provider (or other provider of electronic communication services) to disclose "a record or other information" about a customer or subscriber. 18 U.S.C. § 2703(c). Also, unlike the other provisions of the ECPA, the SCA contains no provisions for its use over an interval of time. *In re Application of U.S. for an Order for Disclosure of Telecommunications Records and Authorizing the Use of a Pen Register and Trap and Trace*, 405 F. Supp. 2d 435, 447 (S.D.N.Y. 2005).

Finally, the Communication Assistance for Law Enforcement Act, 47 U.S.C. § 1002(a)(2), bears mentioning only because a portion of this act relates to the Pen/Trap Statute. CALEA was enacted to ensure that telecommunications carriers maintain adequate technology to allow law enforcement to employ certain investigative techniques, such as wiretaps. It states that the carriers must be able to allow the government to access call-identifying information, "except that, with regard to information acquired solely pursuant to the authority for [PRTT devices], such call-identifying information shall not include any information that may disclose the physical location of the subscriber (except to the extent that the location may be determined from the telephone number)." *Id.* The phrase "solely pursuant to" suggests that, although the Pen/Trap

[7] The full title of this chapter is "Stored Wire and Electronic Communications and Transactional Records Access."

Statute is insufficient to allow the gathering of location data on its own, it may operate in conjunction with another authority to gather location data.

ANALYSIS

Although significant disagreement exists across the legal field regarding how these various authorities apply to technology such as modern cell phones, virtually everyone agrees on one point: The development of modern technology has outpaced the development of statutes and rules governing such technology. Nonetheless, courts must do their best to apply the statutes and rules that do exist to modern technology. In engaging in such an analysis, the Court first considers the "initiate a signal" language the United States asserts it has been submitting in error (but that it nonetheless continues to submit). The Court finds that consideration of the United States' request to order cell phone companies to repeatedly create records by initiating signals is not moot and that the authorities the United States relies on (Rule 41, the SCA, and the Pen/Trap Statute) do not empower the Court to grant such a request.

Second, the Court considers whether the SCA, alone or in conjunction with the Pen/Trap Statute, permits the collection of prospective information as requested in the warrant application at hand. The Court concludes that the "hybrid theory"—the SCA read in conjunction with the Pen/Trap Statute—permits the collection of prospective location information. This conclusion leads to the third inquiry: whether, when used to collect prospective location information under the hybrid theory, a cell phone becomes a tracking device subject to the TDS and the strictures of Rule 41. The Court concludes it does.

I. The authority on which the United States relies does not empower the Court to approve the "initiating a signal" language the United States routinely submits, and the United States' withdrawal of this language from the present warrant does not moot consideration of this issue.

The United States has declined to defend the "initiating a signal" language it routinely and repeatedly submits in the District of New Mexico. Instead, the United States concedes that the submission of this language was a mistake and so has resubmitted the present warrant without this language. Doc. 5 at 2. The United States argues that this withdrawal moots the question of whether requests to initiate a signal are permissible under the SCA. *Id.* At a hearing related to Case No. 1:24-mr-01391-SCY, the United States noted that this "initiating a signal" language is no longer necessary because updated technology now allows for receipt of prospective location information without the extra step of initiating a signal. Case No. 1:24-mr-01391-SCY, Doc. 5 at 9:13-16 ("There is no need for signal initiating in order to collect the data that we are seeking to collect.").

Nonetheless, the "initiating a signal" language merits further discussion because the Government repeatedly submits it to the Court. Over the last ten years, the undersigned has received at least 200 ping warrants containing this language. And over the last two years, a period during which the United States asserts any ping warrants with this language were mistakenly submitted, the undersigned has received dozens of ping warrants with such language. The Court was inclined to rule on the language following the August 1, 2024, hearing in Case No. 1:24-mr-01391-SCY, but accepted the United States' representation that such language would not appear in future warrant applications. Yet, on the following Monday, the Court received another ping warrant application containing the same, oft-repeated, "initiating a signal" language. Based on this history, to include the recent history of the United States submitting such

language even after assuring the Court it had taken measures to prevent future submissions, the Court declines to find the issue moot.

Traditional mootness doctrine takes two forms: constitutional and prudential. Constitutional mootness considers whether "a definite controversy exists throughout the litigation and whether conclusive relief may still be conferred by the court despite the lapse of time and any change of circumstances that may have occurred since the commencement of the action." *Jordan v. Sosa*, 654 F.3d 1012, 1024 (10th Cir. 2011). Prudential mootness, not applicable here, adds a discretionary component to cases involving injunctive or declaratory relief. *See id.*

Two relevant exceptions to the mootness doctrine exist as well. The first, for issues that are "capable of repetition, yet evading review," applies when "(1) the challenged action is in its duration too short to be fully litigated prior to cessation or expiration, and (2) there is a reasonable expectation that the same complaining party will be subject to the same action again." *Brown v. Buhman*, 822 F.3d 1151, 1166 (10th Cir. 2016). The second exception is for "voluntary cessation" and holds that "voluntary cessation of challenged conduct does not ordinarily render a case moot because a dismissal for mootness would permit a resumption of the challenged conduct as soon as the case is dismissed." *Id.*

Neither of these exceptions fit the present circumstances perfectly. In a warrant application, there is no "complaining party," and a warrant application does not involve "challenged conduct" on the part of a defendant. However, the principles underlying these exceptions counsel in favor of ruling on this case. The "initiating a signal" language at issue has appeared regularly in warrant applications before the undersigned for years, and the United

States' assertion that it will cease the use of this language promptly proved inaccurate. In short, the language continues to arise, and the Court finds it prudent to rule.

On the substance of the issue, the analysis is simple. No authority the United States cites says anything about the Court's authority to compel a third-party provider to create records it would not normally create. The SCA permits a governmental entity to "require a provider . . . to disclose a record or other information," § 2703(c), but if a record or other requested information does not already exist, there is nothing to disclose. Similarly, Rule 41 governs search warrants, including warrants for electronically stored information, and it permits "the seizure of electronic storage media or the seizure or copying of electronically stored information." Fed. R. Crim. P. 41(e)(2)(B). The Pen/Trap Statute authorizes "installation and use of a pen register or trap and trace device," 18 U.S.C. § 3123(a)(1), and defines these items as devices capable of recording "dialing, routing, addressing, and signaling information," *id.* § 3127(3), (4), but again, if this information does not exist, there is nothing for these devices to capture. Information that does not yet exist and, absent a court order, will not exist in the future, cannot be seized or copied. Accordingly, the Court holds that the SCA, Rule 41, and the Pen/Trap Statute may not serve as authority for a warrant requiring third-party providers to "initiate a signal" to trigger creation of a record that would not normally be created in the ordinary course of business.

II. Standing alone, the SCA does not empower courts to order cell phone companies to disclose prospective CSLI on a rolling basis.

The SCA's plain text makes clear that it serves as an authority for law enforcement to obtain historical information from cell phone providers. As used in this Opinion, "historical information" means records or other information already in existence at the time the warrant is requested. This is different than the *prospective* location information at issue here. Presently, the United States seeks a warrant that requires a phone company to gather information on a rolling

basis, at all times day or night, for thirty days *after* the warrant is issued.[8] Such authority is not apparent in the SCA, which does not discuss delivery of information on a rolling basis or in real time.

Unable to point to text in the SCA to support its position that the SCA, standing alone, allows law enforcement to use a warrant to obtain prospective records on a rolling basis, the United States pivots to several cases it argues support its position. Even considering these cases, the Court remains unpersuaded.

A. The cases the United States cites either do not support the proposition for which they are cited or are unpersuasive.

Before analyzing the case law the United States cites in its brief (Doc. 5 at 5), the Court notes that only one of these cases is binding Supreme Court or Tenth Circuit precedent. Accordingly, the Court evaluates the rest of the cases only for any persuasive value they might provide.

1. Two cases support a hybrid theory rather than a theory that the SCA by itself provides for mandatory real-time disclosure of prospective information.

In this section of its Opinion (Section II.A), the Court considers only whether the SCA, *standing alone*, permits the collection of real-time prospective location information. A common alternative argument known as the "hybrid approach" considers whether the combined authority

[8] At the September 6 hearing, the Court noted that some judges cross out language in requested ping warrant attachments that require phone companies to provide prospective records on a real-time rolling basis. The United States expressed no interest in seeking a warrant that would provide cell phone companies the option to disclose location information once, at the end of the tracking period. Rather, the United States seeks a warrant in which a provider must furnish records at all times day or night on a rolling basis. At first blush, an order under which a provider would have the option of disclosing records it creates in the ordinary course of business at the end of a short period (fourteen days or less) appears consistent with the text of the SCA and courts' treatment of anticipatory search warrants. Because the United States is not seeking authorization of a warrant under which providers would have such an option, however, the Court does not analyze, or decide, this issue.

of the SCA and the Pen/Trap Statute can justify such a search. Two cases the government cites, *In re Application of the United States for an Order for Prospective Cell Site Location Information on a Certain Cellular Telephone*, 460 F. Supp. 2d 448 (S.D.N.Y. 2006) (Kaplan, J.) and *In re Application of United States for an Order for Disclosure of Telecommunications Records and Authorizing the Use of a Pen Register and Trap and Trace*, 405 F. Supp. 2d 435 (S.D.N.Y. 2005) (Gorenstein, J.), actually endorse the hybrid approach, and not the independent authority of the SCA, for prospective location information collection. Indeed, Judge Gorenstein explicitly rejects the notion that the SCA by itself supplies the necessary legislative authority for such a search: "*Amicus* and the cell site cases have properly pointed to aspects of [§] 2703 that make it unsuited to requiring the carrier to provide cell site data on an ongoing basis." 405 F. Supp. 2d at 447.

In short, although these cases support the idea that the SCA, when combined with the PRTT, empowers courts to authorize ping warrants, they do not support the idea that the SCA alone grants this power. Because these cases support the hybrid theory, the Court will discuss them later, as part of its analysis of the hybrid theory.

2. <u>One case does not address prospective CSLI at all.</u>

The United States cites *In re Applications of U.S. for Orders Pursuant to Title 18, U.S. Code Section 2703(d)*, 509 F. Supp. 2d 76 (D. Mass. 2007) (Stearns, J.). This case took a textual approach in defining the elements of § 2703(c)(1). However, it is of limited value to this discussion: This decision deals solely with historical location information and makes a point to note that prospective information was not requested. *In re Applications*, 509 F. Supp. 2d at 78-79.

3. One case bases its decision on a conclusion with which this Court disagrees—that a cell phone is not a tracking device even when used to monitor a person's movement.

An Eastern District of New York decision, *In re Smartphone Geolocation Data Application*, states that "because a cell phone does not fall within the 'tracking device' exclusion [to the SCA's scope], the Government may properly seek an authorization order for prospective cell site data under [SCA] section 2703." 977 F. Supp. 2d 129 at 150 (E.D.N.Y. 2013). As the beginning of the sentence indicates, this result relies on the conclusion that a cell phone is not a tracking device, a conclusion with which the Court disagrees and which it discusses later in this Opinion. Further, after holding that a cell phone is not a tracking device, the court concludes, with no analysis, "Thus, because a cell phone does not fall within the 'tracking device' exclusion, the government may properly seek an authorization order for prospective cell site data under section 2703." *Id*. at 150. Even if the Court agreed that a cell phone is not a tracking device, it would find this opinion unpersuasive: It contains no citation or analysis to support its conclusion that, if a cell phone is not a tracking device, then the SCA must allow for the recovery of prospective CSLI.[9]

4. One case incorrectly attributes characteristics of ECPA's Title I provisions (governing wiretaps) to ECPA's Title II provisions (the SCA).

The First Circuit's decision in *United States v. Ackies*, primarily considers whether a cell phone, when used to track a suspect's location, is a tracking device. 918 F.3d 190, 199-200 (1st Cir. 2019). *Ackies* concludes that a cell phone is not a tracking device and, as a result, the jurisdictional provision of the SCA, not the TDS, applies to a warrant for location information.

[9] This pre-*Carpenter* case also concludes that individuals hold no reasonable expectation of privacy in their prospective geolocation data, a conclusion *Carpenter* directly rejects. *Compare* 977 F. Supp. 2d at 147, *with* 585 U.S. at 313.

Id. at 198-200. For reasons set forth later in this Opinion, the Court disagrees with this conclusion. Relevant to the present discussion, however, is *Ackies*' brief analysis of whether the SCA allows for continuous monitoring. *Ackies* holds it does. The court writes:

> [the Rule 41] 2006 Advisory Committee Notes differentiate § 3117 from the SCA, stating that the "[u]se of a tracking device is to be distinguished from other continuous monitoring or observations that are governed by statutory provisions or caselaw. See Title II, Omnibus Crime Control and Safe Streets Act of 1968, as amended by Title I of the 1986 Electronic Communications Privacy Act [ECPA]." The SCA is part of ECPA . . . The SCA was a proper basis for the PLI warrants issued here.

Id. at 200 (some citations omitted). The court's logic appears to be as follows: (1) tracking devices are not the only form of continuous monitoring—ECPA lists others; (2) the SCA is part of ECPA; (3) therefore, the SCA must provide for another form of continuous monitoring besides tracking devices.

This logic, however, fails to recognize that ECPA has three distinct titles. Title I, to which the Advisory Committee Notes cite, governs wiretaps. Another part of ECPA, Title III, relates to PRTTs and so provides another form of continuous monitoring distinguishable from location monitoring. In contrast to Titles I and III, which explicitly provide for continuous monitoring, ECPA's Title II—the SCA—does not. Further, nothing in the Advisory Committee Notes indicates that, just because ECPA's Titles I (wiretaps) and III (PRTTs) allow for continuous monitoring, so should Title II (the SCA). Indeed, the 2006 Advisory Committee Notes do not reference Title II (the SCA) at all. The portion of the Notes *Ackies* quotes simply recognizes that tracking people's movement is different than intercepting their phone conversations. This unremarkable recognition says nothing about the character of the SCA—a completely different, and unmentioned, section of ECPA.

In other words, the *Ackies*' rationale is based on a non sequitur. It is true that ECPA has provisions that allow for continuous monitoring—the Advisory Committee Notes cite to wiretap provisions in Title I. It is also true that the Advisory Committee recognized that ECPA's wiretap provisions in Title I provide for monitoring (interception of conversations) that is to be distinguished from the continuous monitoring done through tracking devices. It does not follow from these truths, however, that a completely separate Title of ECPA—Title II (the SCA)—must therefore also provide for continuous monitoring. *Ackies*' rationale for concluding that the SCA allows for continuous real-time location monitoring is, therefore, unpersuasive.

5. One case is irrelevant.

The only Tenth Circuit case on the government's list, *United States v. Mesa-Rincon*, 911 F.2d 1433 (10th Cir. 1990), does not involve the SCA at all; the United States cites to it only in a footnote, observing that "[c]ourts have also approved prospective warrants in other contexts, such as for surveillance video." Doc. 5 at 5 n.4. True enough—*Mesa-Rincon* addresses, and approves, a prospective warrant for video surveillance. In doing so, however, the Tenth Circuit analogizes to the provisions of the wiretap statute and requires compliance with those provisions. *See* 911 F.2d at 1439. Needless to say, the United States does not argue that wiretap prerequisites should apply to warrants for prospective CSLI. *Mesa-Rincon*'s invocation of wiretap protections distinguishes it from the present case.

6. One case addresses anticipatory search warrants, which differ meaningfully from the warrant at issue here.

Also by way of analogy, at the hearing the United States discussed an anticipatory search warrant case: *United States v. All Wire Transactions Involving Dandong Zhicheng Metallic Material Company, Ltd.*, Nos. 17-mj-217 to -224, 2017 WL 3233062 (D.D.C. May 22, 2017) (Howell, J.). Motion Hearing Recording at 2:35:58 (September 6, 2024). This case involves a

search warrant for financial "damming" over a fourteen-day period. *Dandong Zhicheng*, 2017 WL 3233062, at *1. This "damming" process involves freezing all outgoing transactions as well as employing a process to "catch all incoming funds" to an institution, with delivery of the seized funds to law enforcement at the end of the fourteen-day period. *Id.* at *1, *1 n.2. This process essentially functions as an anticipatory search warrant.

Anticipatory search warrants are a well-established part of Fourth Amendment law pursuant to *United States v. Grubbs*, 547 U.S. 90 (2006). Anticipatory search warrants authorize a warrant to be issued if and when a triggering event occurs. In *Grubbs*, the Supreme Court approved of a warrant to search a suspect's home, even when the search could only take place after the suspect accepted a parcel containing child pornography that he had ordered from an undercover postal officer. 547 U.S. at 92-93. It endorsed the two-step logic that once the suspect accepted the package (and there was probable cause he would do so), there would be evidence of a crime in his home, providing probable cause for the search. Similarly, the financial damming case finds probable cause that attempted deposits or withdrawals would occur, as well as probable cause that funds subject to forfeiture would be present in the account, together justifying the warrant for capture and seizure of those funds. *Dandong Zhicheng*, 2017 WL 3233062, at *5.

The case at hand, however, differs from a traditional anticipatory search warrant in meaningful ways. First, the thirty-day timespan of the requested warrant exceeds the fourteen days permitted to complete the execution of a non-tracking warrant. *See* Rule 41(e)(2)(A). Second, anticipatory search warrants do not involve real-time delivery of information on a rolling basis throughout the warrant's timespan. In *Grubbs*, the triggering event was one-and-done: Once the package was delivered, the warrant was executed. In *Dandong Zhicheng*, the

capture of funds was ongoing for fourteen days, but the *delivery* of funds took place in a single discrete event at the expiration of the warrant. 2017 WL 3233062, at *1 n.2 (warrant language included: "Following the expiration of the 14-day period, the financial institution shall immediately effect the seizure of any property collected during this time period via the above directives, and provide such property to a designated law enforcement officer."). To be analogous, the request in this case would need to require the cell phone company to gather information on the suspect's location for a span of fourteen days, then execute the warrant by delivering the information in a single submission to the United States at the end of the fourteen-day timeframe. Were this the case, the United States would have a better argument that such a warrant is not a tracking warrant.

The warrant application in this case, however, essentially seeks to have the warrant executed repeatedly, minutes apart, at all times day or night, for thirty days. Because this is not what happened in *Dandong Zhicheng*, *Dandong Zhicheng* provides little support for the government's argument.

7. *In re Application of the United States for an Order for Authorization to Obtain Location Data Concerning an AT&T Cellular Telephone*, 102 F. Supp. 3d 884 (N.D. Miss. 2015) (Mills, J.)

The final case the United States cites in support of using the SCA alone to gather prospective location information on a rolling basis is *In re Application of the United States for an Order for Authorization to Obtain Location Data Concerning an AT&T Cellular Telephone*, 102 F. Supp. 3d 884 (N.D. Miss. 2015). In connection with an ongoing drug trafficking investigation, the United States sought a search warrant under 18 U.S.C. § 2703(c)(1)(A). *Id.* at 885. "The warrant which the government sought to obtain was a 'prospective' one, which would have compelled phone providers to provide cell phone location data to be generated in the future,

which the government intended to use to track the location of drug suspects." *Id*. The Mississippi court compares the TDS to the SCA and concludes that the SCA is the most effective statutory tool to enforce a warrant for production of prospective cell phone location data. *Id.* at 895. The United States cites to this case for the proposition that "[o]ther courts have generally agreed" that the SCA makes no distinction between prospective and historical information, and therefore, the SCA alone can support a warrant for prospective location information. Doc. 5 at 5.

As an initial matter, it is not clear whether, in this Mississippi case, the United States sought one-time disclosure of prospective information rather than prospective location information on a rolling basis. Indeed, the court may not have resolved this question as it ultimately remanded the case to a Magistrate Judge to determine "what the scope of any warrant authorizing prospective monitoring of cell phone location data should be." *AT&T Cellular Telephone*, 102 F. Supp. at 896. If the court only ordered a one-time production, its decision provides no benefit to the United States' present argument.[10]

The Mississippi court also disagreed with another court's conclusion that the SCA does not provide for disclosure of prospective CSLI. *See id.* at 885 (citing *In the Matter of the Application of the United States of America for an Order Authorizing Prospective and Continuous Release of Cell Site Location Records*, 31 F. Supp. 3d 889 (S.D. Tex. 2014)). The Mississippi court distinguished this case, however, on the grounds that it involved an application for information under § 2703(d), "which imposes a 'specific and articulable facts' standard that requires a considerably lesser showing of proof than the probable cause standard to which the

[10] The court did, however, present hypothetical situations where law enforcement would have an interest in obtaining rolling real-time prospective information. *See id.* at 894 (hypothetical case involving bank robbery suspect fleeing across state lines); *id.* at 895 (hypothetical case involving kidnapper who has taken child out of a particular judicial district). The use of such hypotheticals indicates the warrant at issue may have sought real-time location information on a rolling basis.

government has agreed to subject itself here." *Id*. at 885. The Mississippi court (which did not have the benefit of *Carpenter* at the time it issued its opinion) further stated it was "inclined to agree with" federal courts that did not view cell phone users as having a reasonable expectation of privacy in their location data. *Id*. at 890. It noted, however, that if its inclination was wrong and "prospective cell phone data enjoys Fourth Amendment protection," § 2703(d) *would not* allow law enforcement to obtain prospective cell cite information. *Id*. Unlike the Mississippi court, this Court concludes that prospective cell phone data enjoys Fourth Amendment protection. With this premise, it appears the Mississippi court would agree with the conclusion that § 2703(d) of the SCA *would not* allow law enforcement to obtain prospective CSLI.

Regarding the difference between historical and prospective CSLI, the Mississippi court stated, "It seems to this court that, both as a practical matter and as a constitutional matter, there is no great distinction between historical and prospective cell phone location data." *Id*. at 889. As a practical matter, it noted that "a number of federal courts have found persuasive the 'instantaneous storage theory,' which recognizes that, in the digital age, prospective data instantly becomes stored data, as soon as it is transmitted to a cell phone provider's servers." *Id*.

This theory does have immediate surface appeal. The SCA indisputably allows law enforcement to seize records. Thus, the argument goes, the repeated seizure of CSLI records is really just a repeated exercise of SCA authority. The first problem with this argument is one that has already been discussed—rather than a one-time execution of an anticipatory warrant, such seizure calls for repeated executions of the same warrant for thirty days, at all times day or night.

The second problem with this argument is even more significant. Interpreting the SCA as allowing for the prospective, rolling collection of records creates a backdoor to wiretaps. Location records are not the only types of records obtainable under the SCA. The SCA also

allows the government to obtain a warrant for the content of emails and text messages. 18 U.S.C. § 2703(a). Given that records of a person's location and records of a person's communication are both obtainable under the SCA, no logical reason exists to interpret the SCA as allowing prospective rolling production of the former, but not of the latter. The latter—obtaining records of communications as soon as those records are created on a prospective rolling basis at all times day or night—is, effectively, a wiretap.

Granted, for the reasons the Supreme Court set forth in *Berger v. New York*, 388 U.S. 41 (1967), an interpretation that the SCA allows courts to order such production with nothing more than a warrant likely would not pass constitutional muster. But, if reading the SCA as allowing for the prospective production of records in a way that would effectively circumvent wiretap protections would render the SCA unconstitutional, why would the Court read such a provision into the SCA? *See United States v. Davis*, 588 U.S. 445, 463 n.6 (2019) ("[C]ourts should, if possible, interpret ambiguous statutes to avoid rendering them unconstitutional."). Because (1) the SCA contains no language authorizing the prospective production of records on a rolling basis; (2) reading such a provision into the SCA would render it unconstitutional as applied to wiretaps; (3) no logical reason exists to conclude the SCA allows for rolling production of some records (location information) but not others (content of communications), the Court declines to read such a provision into the SCA.

The Court also disagrees with the Mississippi court's focus on whether the SCA or TDS serves as a better tool for law enforcement. The Mississippi court reasoned, "the Fourth Amendment rights of defendants will be protected regardless" of whether the TDS or SCA serves as the tool to obtain prospective cell site information, and the SCA is a better tool. *AT&T*

Cellular Telephone, 102 F. Supp. at 895. The relevant question, however, is which tool Congress gave to law enforcement, not which tool law enforcement would prefer to have in its toolbox.

Finally, the Mississippi court wrote, "Mechanically speaking, the fact that prospective, rather than historical cell phone data is sought, appears to be of little moment in the context of a technology in which cell phone data is instantly transmitted to and recorded by phone companies." *Id*. That an order to produce prospective information places little burden on phone companies, however, is irrelevant to whether the SCA empowers courts to order phone companies to produce such information. Rather than considering whether any provision in the SCA allows courts to require cell phone companies to provide location information on a rolling basis, the Mississippi court dismisses the difference between production of historical records and production of prospective records as being "of little moment" given that cell phone companies can provide prospective information just as easily as historical information. The Court disagrees with the assessment that the difference is of little moment.

Finally, post-*Carpenter*, we know that the Supreme Court has rejected the view of the Mississippi court and numerous other district courts at the time that cell phone possessors have no reasonable expectation of privacy in their cell phone location information. Further, we know that the Supreme Court's focus in *Carpenter* was on the privacy interests of the cell phone holder, not on the burden that search warrants would impose on cell phone companies. *Carpenter*, therefore, eroded the foundation on which the Mississippi court's decision was based. Further, the Mississippi court's rationale that it is just as easy for cell phone companies to provide prospective cell phone location information as it is to provide historical information does not answer the question of what provision in the SCA allows courts to order cell phone companies to disclose real-time location information on a rolling basis for more than a fourteen-

day period. In the absence of such analysis, the Mississippi court's decision does not advance the United States' argument.

B. Numerous district court cases have concluded that the SCA on its own cannot support a warrant for the production of prospective CSLI on a rolling basis.

Standing against the cases the United States cites are numerous district court opinions that have concluded the SCA on its own cannot support a warrant for the production of prospective CSLI on a rolling basis. These decisions largely reject this notion for the same reason as this Court: Nothing in the SCA provides courts with this power. *See In re Authorizing the Use of a Pen Register*, 384 F. Supp. 2d 562, 563-64 (E.D.N.Y. 2005), reconsidered by *In re Application of the United States for an Order Authorizing the Use of Pen Registers and Trap/Trace Device and Authorizing the Release of Subscriber Information and/or Cell Site Information*, 396 F. Supp. 2d 294 (E.D.N.Y. 2005); *In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority*, 396 F. Supp. 2d 747, 758-60 (S.D. Tex. 2005); *In re Application of the U.S. for Orders Authorizing the Installation and Use of Pen Registers and Caller Identification Devices on Telephone Numbers [Sealed] and [Sealed]*, 416 F. Supp. 2d 390, 395 (D. Md. 2006) (rejecting both use of SCA alone to obtain prospective information and hybrid approach with Pen/Trap Statute); *Matter of Search of Cellular Tel.*, 430 F. Supp. 3d 1264, 1272-74 (D. Utah 2019) (concluding ping warrant requires All Writs Act order).[11]

C. Conclusion

The Court finds no language in the SCA that empowers it to order the collection of records on a rolling, real-time basis and the cases the United States cites points to no such

[11] Although most of these cases were decided before 2018, when the Supreme Court decided *Carpenter*, their analysis does not conflict with *Carpenter*.

language. In contrast, consistent with the Court's analysis above, numerous cases persuasively hold that the SCA does not provide courts such power. Consequently, the Court concludes that the SCA does not, on its own, authorize search warrants for prospective, rolling CSLI.

III. "Hybrid theory": The SCA can combine with the Pen/Trap Statute to allow collection of prospective location information.

Various courts have suggested that, even though the SCA alone cannot support the rolling transmission of prospective location information, it can do so in conjunction with the Pen/Trap Statute. Briefly, the logic is as follows. The Pen/Trap Statute allows for ongoing gathering of prospective information (phone numbers and other similar call-identifying information). For its part, CALEA, 47 U.S.C. § 1002(a)(2), states that information gathered "solely pursuant to" the Pen/Trap Statute "shall not include any information that may disclose the physical location of the subscriber." The "solely pursuant to" language suggests that the Pen/Trap Statute can work in conjunction with another statute to gather information about the subscriber's physical location.

So far, so good. But, although Congress incorporated this "solely pursuant to" language into CALEA, it did not clarify *which* authority might combine with the Pen/Trap Statute to empower courts to authorize ping warrants. The United States argues, with support from various district court decisions, that the addition of a search warrant obtained under § 2703 of the SCA does the trick. *See, e.g.*, *In re Application of the United States for an Order for Prospective Cell Site Location Information on a Certain Cellular Telephone*, 460 F. Supp. 2d 448 (S.D.N.Y. 2006) (Kaplan, J.); *In re Application of United States for an Order for Disclosure of Telecommunications Records and Authorizing the Use of a Pen Register and Trap and Trace*, 405 F. Supp. 2d 435 (S.D.N.Y. 2005) (Gorenstein, J.); Doc. 5 at 11-12.

The authors of these opinions raised concerns about choosing a statute to combine with the Pen/Trap Statute in light of Congress's silence on the matter. *See Certain Cellular Telephone*,

460 F. Supp. 2d at 461 (lack of direct authorization to combine statutes is "somewhat troubling" for hybrid approach, but ultimately not fatal); *Disclosure of Telecommunications Records*, 405 F. Supp. 3d at 443-44 (hybrid approach is "certainly an unattractive choice" given lack of Congressional guidance, but is ultimately "the only choice possible"). Combining two statutes that do not reference each other to create a new authority to issue ping warrants when neither statute could authorize them on its own involves a degree of improvisation that unsettles the Court. Courts are in the business of interpreting laws, not creating new ones, so the Court would not be inclined to recognize such a novel and far-reaching combination without some indication in the structure and plain text of applicable statutes that Congress intended such a creation. In this case, however, the structure of ECPA and the plain text of CALEA do provide such indication.

ECPA recognizes a continuum. The more intrusive the government action, the more procedural protections and court oversight are required. On one end of the spectrum are wiretaps. The Supreme Court in *Berger v. New York* recognized that real-time interception of citizens' private conversations approaches the zenith of government intrusion. 388 U.S. 41 (1967). Not even a search warrant, supported by a neutral judge's probable cause finding of criminal activity, is sufficient to justify such an intrusion. Before obtaining a court order, the government must establish the details of the offense and the types of communications to be intercepted, exhaustion of other investigative techniques, and a statement of the time period for which interception will take place. 18 U.S.C. § 2518. The government must also minimize the interception of communications not covered by the wiretap order. *Id*. Finally, like other statutes allowing for the prospective collection of information, ECPA's wiretap provisions limit the duration of the interception. *Id.* § 2518(5).

At the other end of the spectrum are PRTT orders, which essentially allow the United States to obtain dialing, routing, addressing, and signaling information—largely, phone numbers of incoming and outgoing calls. 18 U.S.C. § 3121(c). PRTT orders do not allow the United States to obtain content and, by themselves, cannot be used to obtain location information. Accordingly, the threshold for obtaining a PRTT order is low. Law enforcement need only certify the relevance of the information they seek to an ongoing criminal investigation. 18 U.S.C. § 3122(b)(2).

Between these extremes is prospective CSLI. Tracking a person's location is more intrusive than learning who a person has been talking to on the phone, but less intrusive than listening to or reading a person's purportedly private conversations. In *Carpenter*, the Supreme Court recognized historical CSLI's place on the continuum. There, the Supreme Court held that "accessing seven days of CSLI constitutes a Fourth Amendment search." *Carpenter*, 585 U.S. at 310 n.3. That is, the United States must show less to obtain a warrant under the SCA for seven days of historical CSLI than to obtain an order allowing it to intercept a person's private conversations. To obtain other historical records under the SCA, however, the United States need not even obtain a warrant. *See* 18 U.S.C. § 2703(d) (allowing a court to order production of records when "a governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation"). Although prospective CSLI might be farther toward the wiretap end of the continuum, it is well established that no more than a warrant is needed to obtain real-time prospective location information. Fed. R. Crim. P. 41(e)(2)(C) (relating to warrants for tracking devices).

Thus, the Supreme Court recognizes that the Fourth Amendment does not bar real-time interception of phone conversations. And when the government obtains an order authorizing such interception, Congress requires phone companies to furnish "forthwith all information, facilities, and technical assistance necessary to accomplish the interception . . . ." 18 U.S.C. § 2518(3)(e). Given this, it would be anomalous to carve out production of prospective location information from phone companies as entirely inaccessible. That is, recognizing that mechanisms exist to obtain historical cell cite information *and* even more intrusive wiretap information, it would be odd that no mechanism exists for law enforcement to obtain prospective cell site location information.

Moreover, and crucially, it appears that Congress intended for such a mechanism to exist. Consider CALEA, which Congress enacted to ensure that electronic communications providers maintain technology that allows for investigative techniques such as wiretaps. As part of CALEA, and in recognition that numbers dialed and numbers received no longer constitute the universe of signals that phones receive, Congress updated the language of the PRTT to include call routing and addressing information. *See* 18 U.S.C. § 3121 (2021 Amendment). This change prompted concerns that a PRTT order (which, as noted, has a very low threshold for authorization) could be used to obtain location information. *See In re Application of the United States of America for an Order Authorizing the Release of Prospective Cell Site Information*, 407 F. Supp. 2d 134, 137-38 (D.D.C. 2006) (testimony of FBI Director Louis Freeh regarding such concerns). Congress thus included a restriction: information gathered "solely pursuant to" the Pen/Trap Statute "shall not include any information that may disclose the physical location of the

subscriber." 47 U.S.C. § 1002(a)(2).[12] The use of the phrase "solely pursuant to" indicates that the Pen/Trap Statute can be combined with something else to obtain location information.

Although Congress chose not to specify the something else (or the something elses) that can be combined with the PRTT to obtain real-time prospective cell site location information, the SCA seems the likeliest contender. The SCA allows for disclosure of historical location information pursuant to *Carpenter*. Meanwhile, the Pen/Trap Statute allows for the rolling delivery of prospective information—albeit not location information—that the SCA cannot provide on its own. Together, they appear to fill in each other's gaps,[13] and cover rolling, prospective location information.

Based on this reasoning, the Court concludes that the hybrid approach is a permissible means of obtaining a warrant for prospective cell phone location information.

---

[12] A debate exists regarding what meaning can be gathered from the legislative history that led to the insertion of the phrase "solely pursuant to" into CALEA's PRTT provisions. This debate analyzes the testimony of Director Freeh and the timing of Congress' insertion of this phrase "solely pursuant to" into CALEA. *Compare In re Application of United States for an Order for Disclosure of Telecommunications Records and Authorizing the Use of a Pen Register and Trap and Trace*, 405 F. Supp. 2d 435, 443 (S.D.N.Y. 2005), *with In re the Application of the United States for an Order Authorizing the Disclosure of Prospective Cell Site Info.*, 412 F. Supp. 2d 947, 955-56 (E.D. Wis. 2006). The Court declines to engage in this debate. Rather than focusing on the legislative process that led to certain text and then attempting to divine meaning from that process, the Court instead chooses to focus on the plain language that came out of that legislative process.

[13] CALEA's "solely pursuant to" language applies to the Pen/Trap Statute only as it relates to location information. Thus, in enacting CALEA, Congress did not open the door to the Pen/Trap Statute combining with some other statute for any law enforcement technique other than the gathering of location information. Attempts to obtain prospective other-than-location-records by combining the SCA and Pen/Trap Statute are therefore doomed. CALEA only blesses location records with its "solely pursuant to" caveat.

IV. Cell phones are tracking devices subject to the procedural requirements of Rule 41.

The Court next considers whether a cell phone should be considered a tracking device under Rule 41. This classification matters for two reasons. First, targets of a tracking device enjoy certain procedural protections. Once a court signs a tracking device warrant, agents have ten days to "complete any installation authorized by the warrant" whereas agents have fourteen days to execute a warrant to search for or seize property. *Compare* Fed. R. Crim. P. 41(e)(2)(C)(i), *with* Fed. R. Crim. P. 41(e)(2)A)(i). More significantly, unless the agent who obtains a tracking warrant gets an extension under Rule 41(f)(3), Rule 41(f)(2)(C) requires the agent to serve a copy of the tracking warrant on the person tracked within ten days after the use of the tracking device has ended.

Second, the jurisdictional provision that applies to the installation of a tracking device is not as broad as the jurisdictional provision in the SCA. The TDS requires the tracking device to be installed in the same district where the warrant is obtained (18 U.S.C. § 3117(a)), whereas the SCA allows a judge to issue a warrant for SCA records that are contained in a different jurisdiction, as long as that judge's district "has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3). Consequently, the United States' interpretation that the cell phone does not qualify as a tracking device allows it to avoid the narrower jurisdictional provision of the TDS.[14]

[14] If the United States' argument that ping warrants require no installation is correct, however, the TDS's jurisdictional provision, which only relates to installation of the device, may not be implicated. This would be true even if a cell phone is defined as a tracking device when used to track a suspect's movement. *See* 18 U.S.C. § 3117(a). Although defining a cell phone as a tracking device would still implicate Rule 41 provisions related to tracking devices, the absence of an installation likely means the TDS's jurisdictional provision is never invoked. Nonetheless, as explained in more detail below, the United States' ping warrant applications specifically request an installation. The United States' request for an installation and proposed order calling for an installation makes it difficult for the United States to credibly argue that what needs to be done to enable law enforcement to track suspects through their phones requires no installation.

The Court recognizes that defining a device the United States uses to track a person's movements as a tracking device comes with procedural and jurisdictional downsides. Inconveniences that result from a statute's application, however, cannot change the nature of a device or the plain meaning of a statutory definition. *See Borden v. United States*, 593 U.S. 420, 436 (2021) ("A court does not get to delete inconvenient language and insert convenient language to yield the court's preferred meaning."). Similarly, a court does not get to delete inconvenient language and insert convenient language to yield the government's preferred meaning. *See Bostock v. Clayton Cnty., Ga*., 590 U.S. 644, 673-74 (2020) ("This Court has explained many times over many years that, when the meaning of the statute's terms is plain, our job is at an end. The people are entitled to rely on the law as written, without fearing that courts might disregard its plain terms based on some extratextual consideration.").

A. When used to track a person's movements, cell phones meet the statutory definition of tracking devices.

The TDS defines a "tracking device" as "an electronic or mechanical device which permits the tracking of the movement of a person or object." 18 U.S.C. § 3117(b). When used to track a person's movements, a cell phone clearly fits this definition—it is an electronic device that permits the person carrying it to be tracked. Here, the United States seeks "information about the location of the Target Cell Phone" for the purposes of monitoring the suspect's movements twenty-four hours a day over a thirty-day period. Doc. 8 at 14 (Ping AO106a, Attachment B). That is, a ping warrant enables the United States to use a person's cell phone (an electronic device) to track that person's movement. In such instance, the cell phone and the United States' use of it precisely fit the definition Congress enacted for a tracking device ("an electronic or mechanical device which permits the tracking of the movements of a person or object"). 18 U.S.C. § 3117(b). This should be the end of the story.

But a clear fit between the device, its use, and the statutory definition is not the end of the story for the United States. Rather, the United States argues that the jurisdictional section of the TDS modifies the definitional section. The jurisdictional section states, "If a court is empowered to issue a warrant or other order for the installation of a mobile tracking device, such order may authorize the use of that device within the jurisdiction of the court, and outside that jurisdiction if the device is installed in that jurisdiction." 18 U.S.C. § 3117(a). Because this jurisdictional provision refers to installation, the United States argues that suspects' cell phones, which agents do not physically install, cannot be tracking devices. Doc. 5 at 6.

None of the arguments the United States makes in support of its interpretation of the TDS adequately explain why, when the TDS's definition of a tracking device is clear and unambiguous, the Court should reach over to the TDS's unrelated jurisdictional provision to modify this clear and unambiguous definition. Nor do its arguments explain how the Court could do so without violating the Supreme Court's admonitions in *Borden* and *Bostock*.

Instead, the United States asserts that the TDS "applies only when a court is authorized to issue an order 'for the installation of a mobile tracking device,' . . ." Doc. 5. But why should this be the case? The TDS's jurisdictional provision is really just a codification of a point the Supreme Court later recognized in *Jones*—if a tracking device must be installed, it must be installed in the district where the warrant is obtained. *United States v. Jones*, 565 U.S. 400, 402-03 (2012) (observing that the United States did not contest that the installation of a tracking device in the District of Maryland, when the tracking device warrant was issued in the District of Columbia, rendered the warrant invalid). That an electronic device used to track movement needs no installation provides no justification for ignoring the plain language of § 3117(b) and calling that device something other than a tracking device. Accordingly, the Court defers to Congress'

definition of a tracking device and declines to place limitations on this definition that Congress did not.

B. The United States' legislative history argument is unpersuasive.

The United States cites to ECPA's legislative history in support of its position that, rather than applying the clear and unambiguous language Congress used to define a tracking device, the Court should import words from an unrelated section. It asserts that "Congress understood 'tracking devices' to be government-installed homing devices rather than cellular telecommunication technologies." Doc. 5 at 7. This statement is probably true. But it is not surprising that, in 1986 when Congress enacted ECPA (to include the TDS), it did not explicitly address devices not yet invented (modern day cell phones with tracking capabilities). Nor does this mean that the broad language Congress did choose fails to account for not-yet-invented modes of tracking, such as signals from cell phones.

To be sure, as the United States points out, Congress has since amended other portions of ECPA to account for changes in technology, such as the advent of smartphones. *See* Doc. 5 at 8. But because the TDS's definition of a tracking device already encompasses smartphones, Congress has had no reason to update the language in § 3117(b) to encompass smartphones. That Congress has not updated a statute that needs no updating is no reason to read the words of that statute differently than what they plainly mean.

C. *Ackies* is unpersuasive.

The Court recognizes that the United States' position is consistent with that of the First Circuit. In *Ackies*, the First Circuit rejected a defendant's argument that "a cell phone used to track a person's movements is a 'tracking device' under 18 U.S.C. § 3117 . . . ." 918 F.3d 190,

198. For the following reasons, this Court believes that the proper statutory analysis compels a different conclusion.

First, like the United States in its brief, *Ackies* assumes without explanation that the TDS's jurisdictional provision alters its definitional provision. As set forth above, this Court disagrees. The absence of a need to install a tracking device and the consequent absence of a need to invoke the TDS's jurisdictional provision do not change the nature of the electronic device being used to track a person's movement or change the definition of a tracking device.

Second, *Ackies* concludes that "§ 3117 does not work when considering cell phone location data, because it could be exceedingly difficult in situations involving [precision location information] to determine where installation is to occur and the government may be seeking data concerning a cell phone whose present location is unknown." *Id*. at 199 (internal quotations and citation omitted). As set forth in more detail below, concerns that application of § 3117's jurisdictional provision to ping warrants would significantly impair the United States' ability to obtain such warrants are overblown. Regardless, Supreme Court precedent does not allow courts to alter the words of a statute because some different meaning would be more convenient for the government. *Borden*, 593 U.S. at 436; *Bostock*, 590 U.S. at 673-74.

Third, *Ackies* addresses the Advisory Committee Notes for Rule 41(e)(2)(C), which governs warrants for tracking devices:

> The Advisory Committee Notes for the 2006 Amendments to the Rules state that a "magistrate judge's authority under [the tracking device warrant] rule includes the authority to permit ... installation of the tracking device, and maintenance and removal of the device." Advisory Committee's Notes on 2006 Amendments to Fed. R. Crim. P. 41 (emphasis added). There is no "maintenance" or "removal" of a "device" when gathering precise location information from a cell phone.

Id. at 199-200. True enough. A magistrate judge's powers *include* the ability to permit maintenance and removal of the device. That Rule 41 provides magistrate judges with power

they may sometimes, but not always, need to use, however, is unremarkable. Just because a rule provides a magistrate judge authority the judge does not need in a particular instance is no reason to change the plain meaning of a Congressional statute.

Fourth, *Ackies* reasoned:

> [the Rule 41] 2006 Advisory Committee Notes differentiate § 3117 from the SCA, stating that the "[u]se of a tracking device is to be distinguished from other continuous monitoring or observations that are governed by statutory provisions or caselaw. See Title II, Omnibus Crime Control and Safe Streets Act of 1968, as amended by Title I of the 1986 Electronic Communications Privacy Act [ECPA]." The SCA is part of ECPA . . . The SCA was a proper basis for the PLI warrants issued here.

Id. (some citations omitted). Here, *Ackies* points out that tracking a person's movements is different than intercepting their phone conversations. But this truth provides no reason to change the definition Congress gave to the term "tracking device."[15]

Fifth, *Ackies* observes that the SCA allows the United States to obtain warrants for location information. Yet, *Ackies* did not address whether, or how, the SCA allows the United States to obtain prospective, real-time location information on a rolling basis. Nonetheless, to the extent a § 2703(c)(1)(A) warrant is used in conjunction with a PRTT order, the Court agrees that the SCA (via § 2703(c)(1)(A)) provides a means for the United States to obtain real-time CSLI. Again, however, the ability to obtain records under the SCA (whether alone as some courts may conclude or in conjunction with the Pen/Trap Statute as this Court concludes) provides no reason to change the definition Congress gave to the term "tracking device."[16]

---

[15] The Court addressed *Ackies*' conclusion that "[t]he SCA was a proper basis for the PLI warrants issued here[,]" *id*. at 200, in section II.A of this Opinion.

[16] As explained above, if the United States could obtain real-time CSLI without the need for an installation, it would have a strong argument that the TDS's jurisdictional provision would not be invoked and that the SCA's jurisdictional provision should apply. However, where the United

D. Categorizing cell phones as tracking devices when they are used to track a person's movement does not lead to absurd results.

Next, the United States argues that defining a cell phone as a tracking device would lead to absurd results. Doc. 5 at 8-9. The Court disagrees and addresses each putative absurd result below.

1. Applying § 3117(b) to cell phones used to track a person's movement will not eviscerate heightened wiretap protections.

The government claims that characterizing cell phones as tracking devices would exclude cell phone conversations, text messages, and emails from the protection of wiretap statutes. Doc. 5 at 8. Its argument begins with the definition of "electronic communication" found in ECPA's wiretap provisions. Those provisions codify the heightened protections, which are beyond those of a mere search warrant, that the Supreme Court in *Berger* held shall apply when the United States intercepts a suspect's telephone communications. 388 U.S. at 58-60. Although email and text messages did not exist in 1967 when the Supreme Court decided *Berger*, these heightened protections not surprisingly also apply to the real-time interception of emails and text messages. Also not surprisingly, Congress and the Supreme Court have not equated the intrusion of privacy that occurs when the government intercepts a person's private phone communications with the

States seeks records under the SCA *and* an installation under the TDS, the jurisdictional provisions of the SCA and the TDS come into tension. Which jurisdictional provision should apply? The United States does not argue that the SCA's jurisdictional provision should trump the TDS's jurisdictional provision where records are sought under the SCA and an installation occurs under the TDS. To the contrary, among the reasons the United States argues the Court should not define a cell phone as a tracking device is that doing so would require the United States to comply with the TDS's jurisdictional provision rather than SCA jurisdictional provision. *See* Motion Hearing Recording at 2:12:20, 2:20:30 (September 6, 2024) (asserting that, if a cell phone is defined as a tracking device, the TDS's jurisdictional provision would apply and this would impair law enforcement's ability to locate dangerous criminals). Consequently, whether the TDS's jurisdictional provisions apply in cases where an installation is involved in the process of rendering a cell phone a tracking device is not presently at issue.

intrusion of privacy that occurs when the government tracks a person's location. *Compare id.* (requiring a particular description of conversations sought, termination date for interception period, and showing of exigency, among other procedures), *with Carpenter*, 585 U.S. at 316 (requiring a warrant supported by probable cause to obtain historical CSLI records). Consequently, the heightened protections the Supreme Court and Congress have attached to wiretaps do not apply to location tracking.

The definitional section of ECPA's wiretap provisions makes this clear. It states that although the "electronic communication" covered by ECPA's wiretap provision generally includes the transfer of signals, it does not include "any communication from a tracking device (as defined in section 3117 of this title)." 18 U.S.C. § 2510(12)(C). So far, this makes sense—obtaining a cell phone's tracking signals is less intrusive than intercepting a conversation and so the heightened protections associated with wiretaps do not apply to cell phone tracking. The next part of the United States' argument is more difficult to follow.

The Court understands the United States' argument to be as follows: (1) assume a cell phone is a tracking device; (2) now apply § 2510(12)(C); (3) § 2510(12)(C) says "any communication" from a tracking device is not covered by ECPA's wiretap provisions; (4) because a cell phone is a tracking device its communications are not covered by ECPA's wiretap provisions; (5) conversations on cell phones are communications; (6) thus, defining a cell phone as a tracking device exempts conversations on cell phones from heightened protections ECPA put in place to cover wiretaps. In short, the government says calling a cell phone a tracking device means that cell phone communications are immune from wiretap protections. Doc. 5 at 8.

The United States' position, however, fails to recognize that many uses of a cell phone do not permit the tracking of the movement of a person or object. As the Supreme Court recognized

in *Riley v. California*, cell phones "could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers." 573 U.S. 373, 393 (2014). Indeed, affidavits for cell phone searches routinely avow that cell phones can function as cameras and electronic storage devices. The Court agrees. When a cell phone is taking pictures, it is a camera, not a tracking device. When it is shining a light, it is a flashlight, not a tracking device. When it is used to audio-record, it is a recorder, not a tracking device. When it is used to engage in conversations, it also is not a tracking device. And when a cell phone is used to converse or surreptitiously record a conversation, and not used as a tracking device, interceptions of those conversations are subject to ECPA's wiretap provisions. In contrast, when the signals a cell phone sends are only used to transmit location data, it functions as a tracking device and it is not subject to the heightened protections of wiretap statutes. Thus, § 2510(12)(C) does not apply to tracking-related communications from a cell phone and those signals are not subject to the provisions of the wiretap statute. Content-related communications from the same device, on the other hand, fall squarely within the protections of § 2510(12)(C).[17]

The Advisory Committee Notes to Rule 41 support this conclusion. In relevant part, these notes state, "Use of a tracking device is to be distinguished from other continuous monitoring or observations that are governed by statutory provisions or caselaw." Advisory Committee Notes on 2006 Amendments to Fed. R. Crim. P. 41 (citing Title III, Omnibus Crime Control and Safe Streets Act of 1968, *as amended* by Title I of the 1968 Electronic Communications Privacy Act, 18 U.S.C. §§ 2510-2520). In this way, the Advisory Committee recognized that tracking is

[17] The Court agrees with the reasoning of two cases that discuss this § 2510(12)(C) issue in more detail. *In re Application of United States for an Order Authorizing the Use of Two Pen Register & Trap & Trace Devices*, 632 F. Supp. 2d 202, 207 (E.D.N.Y. 2008), and *In re Application of the U.S. for an Order Authorizing the Disclosure of Cell Site Location Info.*, No. 6:08-6030M-REW, 2009 WL 8231744, at *7 (E.D. Ky. Apr. 17, 2009).

different than wiretapping. Although cell phones can emit both communication signals that can be intercepted and other signals that provide location, the emission of signals that lead to tracking location is to be distinguished from the emission of signals that lead to the interception of conversations.

A hypothetical the Court posited at the September 6 hearing also illustrates the deficiency in the United States' argument. Suppose an undercover agent conducts a controlled buy of narcotics in the back of a suspect's car. Wanting to track where that car goes next, the agent wedges a cell phone between the cushions of the back seat so that he can use one of the many applications on the market to track the phone and, with it, the movement of the suspect's car. Would the cell phone wedged in the back seat cushions be considered a tracking device? It is an electronic device that tracks the movement of an object and one the agent installed by wedging it between the back seat cushions of the car. At the September 6 hearing, the United States agreed that, in such a situation, the cell phone would meet the definition of a tracking device and would require a tracking warrant. Motion Hearing Recording at 1:41:11 (September 6, 2024).

But consider the implications of accepting the United States' argument that, if a court defines a cell phone as a tracking device, application of § 2510(12)(C) excludes interception of that phone's communications from wiretap protections. Under the government's argument, because the cell phone has acted as a tracking device, § 2510(12)(C) immunizes interception of that phone's communications from ECPA's heightened wiretap protections. Before placing the phone in between the cushions, the agent could call a fellow agent and leave the line open. Or, the agent could hit the record button on an app that allows recordings to be accessed remotely. Agents could then listen to, and record, whatever the drug-dealing suspect(s) might say upon

driving away from the controlled buy. And, accepting the government's argument, they could do so without the need to abide by ECPA's provisions governing wiretaps.

We know, however, that if this hypothetical came to life, the United States would not actually argue that § 2510(12)(C) would allow it to use the cell phone to legally intercept conversations without a wiretap order. We know this because United States asserts doing so would be absurd. Doc. 5 at 8 ("[A]s a practical matter, finding cellular phones to be 'tracking devices' would lead to absurd results. First text messages and emails sent from cellphones would not be 'electronic communications' under the Wiretap Act, and their interception would no longer be prohibited." (citing 18 U.S.C. §§ 2511(1)(a) (prohibiting interception of electronic communications), and *id.* § 2510(12)(C) (excluding 'any communication from a tracking device' from the definition of an 'electronic communication')). The United States, of course, made this statement as part of its argument that ping warrants require no installation and so cannot be defined as tracking devices.

As the Court's hypothetical demonstrates, however, realistic circumstances exist where agents might physically install a cell phone they then use to track a suspect's movement. The United States acknowledges that the cell phone in the Court's hypothetical, having been physically installed, would have to be defined as a tracking device. Applying the United States' argument that § 2510(12)(C) exempts cell phones from wiretap requirements when they are defined as tracking devices would allow agents to obtain a warrant, physically install a cell phone on a suspect's property, and then, because communications from tracking devices are exempt from ECPA's wiretap requirements, surreptitiously listen to the suspect's conversations

without the need to comply with wiretap requirements.[18] The Court agrees with the United States that such an interpretation is absurd. The absurdity arises, however, not because the United States' assertion that cell phones can never be considered tracking devices is correct. Instead, the absurdity arises because the United States' assertion that defining cell phones as tracking devices exempts their communications from wiretap requirements is incorrect.

2. Broad application of § 3117(b) does not lead to absurd results.

The United States also asserts that if a cell phone's "capability to emit geolocation information converted it into a 'tracking device' under § 3117[(b)], nearly all modern technologies would become 'tracking devices' when used to convey information about a user's location, including pagers, ATMs, retail credit-card terminals, landline telephones, and most IP-connected technologies." Doc. 5 at 8-9. But while ATMs, retail credit-card terminals, landline telephones, and most IP-connected technologies can provide a person's location at one moment in time, they do not continuously track a person's movement and so do not fit the definition of a tracking device.[19] As for pagers, to the extent those devices emit a signal that allows law enforcement to track the movement of persons carrying them, nothing is absurd about also defining pagers as tracking devices.

Of course, many other common electronic or mechanical devices are mobile and can be used to track a person's movement. *See In re Smartphone Geolocation Data Application*, 977 F.

[18] Although this might allow law enforcement to circumvent ECPA's wiretap provisions, such conduct would still be illegal under *Berger v. New York*, 388 U.S. 41 (1967).

[19] At oral argument, the United States noted that a system of fixed cameras could track a person's movement. Motion Hearing Recording at 1:52:20 (September 6, 2024). True, one can envision an Orwellian world where the government's system of stationary cameras and monitoring devices is so sophisticated that it could track a person's every movement for an extended period. In such a world, stationary cameras might qualify as tracking devices. This result would not be absurd, however.

Supp. 2d 129 (E.D.N.Y. 2013) (under a broad reading of § 3117(b), bike tracks in a muddy field or automobile taillights could qualify as tracking devices). But that does not mean concluding such devices fit the definition of a tracking device leads to absurd results. Take an automobile taillight. What is the effect of defining it as a tracking device? If the United States is not seeking a search warrant, that a device falls within the definition § 3117(b) means nothing. There is no effect—and no absurd result—from such categorization.

Granted, it would be absurd if defining a taillight as a tracking device meant law enforcement would have to obtain a search warrant to follow the car displaying the taillight on public thoroughfares. But that is not the case. As the Supreme Court recognized in *United States v. Jones*, "This Court has to date not deviated from the understanding that mere visual observation does not constitute a search." 565 U.S. 400, 412 (2012). Thus, following a car's taillights on public thoroughfares does not require a search warrant, does not implicate Rule 41's provisions, and so does not lead to any result, absurd or otherwise. That Rule 41 contains procedures related to tracking devices that apply when warrants are required does not mean that every use of a tracking device requires a warrant.

Take, for instance, the beeper at issue in *United States v. Knotts*, 460 U.S. 276 (1983). Before a container came into a suspect's possession, law enforcement, without a warrant, installed a beeper on the container. *Id*. at 278-79. After the container came into the suspect's possession, law enforcement, without a warrant, used signals from the beeper to track the suspect's movement. *Id*. Thus, the beeper at issue in *Knotts* would neatly fall within even the United States' proffered definition of a tracking device—it is an electronic device that an agent installed and that is used to track the movement of a person or object. That a beeper like the one used in *Knotts* fits the definition of a tracking device, however, has no legal relevance. As the

Supreme Court held, using that beeper for limited tracking did not constitute an illegal warrantless search because "[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another." *Id*. at 281.

Knotts demonstrates that not every use of every tracking device requires a search warrant. When no search warrant is sought, Rule 41's tracking device procedures are not invoked and so are not relevant. Defining a taillight as a tracking device only seems absurd if one wrongfully assumes that law enforcement would need a warrant to follow that taillight on a public thoroughfare. The absurdity comes only from requiring a search warrant in situations where one is not needed. The United States provides no example where defining an electronic or mechanical device that tracks the movement of a person or object would be absurd under circumstances where a warrant is needed.

In sum, although it might be nonsensical to require law enforcement to obtain a search warrant to follow tire tracks or a car's taillight, no part of the TDS or Rule 41 compels that result. The only time the definition of a tracking device matters is when that tracking device intrudes upon a person's reasonable expectation of privacy, triggering the warrant requirements in Rule 41 (and associated protections for individuals against whom a tracking device is used). Otherwise, whether a device fits within the definition of a "tracking device" has no practical consequence. The result of a broad interpretation of § 3117(b) is not absurd.

Finally, even if a creative person could think of some far-fetched hypothetical in which an application of § 3117(b) would lead to an absurd result, this would not justify a refusal to apply § 3117(b)'s unambiguous definition as it pertains to the non-hypothetical, real-world ping warrant presently at issue. A "parade of horribles" may not "surmount the plain language of [a] statute." *Truck Ins. Exch. v. Kaiser Gypsum Co., Inc.*, 602 U.S. 268, 284 (2024).

3. The parade of horrible consequences the United States presents is overstated.

And the United States does present a parade of horribles. It worries that defining a cell phone as a tracking device when subject to a ping warrant will produce a series of unfortunate consequences. Even if the government's parade of horribles were relevant to the Court's interpretation of § 3117(b), however, the government's concerns are overstated. Defining a cell phone as a tracking device when it is used to track a person's movement is unlikely to severely impair law enforcement's investigatory capabilities.

a. Use of the TDS's jurisdictional provision is unlikely to significantly impair law enforcement's ability to obtain tracking device warrants.

At the September 6 hearing, the United States seized on a factual scenario the Mississippi court (discussed in section II.A above) presented to demonstrate a need to obtain prospective cell site information under the SCA. Motion Hearing Recording at 2:12:20 (September 6, 2024). The case involved a bank robbery in December 2013. *AT&T Cellular Telephone*, 102 F. Supp. 3d at 894. The robbery took place in Tupelo, Mississippi, and led to the death of one police officer and the critical injury of another. *Id*. According to law enforcement, the same person had robbed a bank in Atlanta, Georgia, the day before. *Id.*

The United States sought cell tower information from locations near both banks and the major transportation routes between them. *Id*. Pursuant to the TDS, "only a court in the jurisdiction where the phone is located can issue the warrant." *Id*. Officers did not know where the phone was located. *Id.* But § 2711(3) of the SCA allows any court with jurisdiction over the offense being investigated to issue a warrant for records obtainable under the SCA. *Id.* Thus, if § 2711(3) applied, the United States could obtain a search warrant "without regard to the location

of the cell phone."[20] *Id.* In the present case, the United States argues that, without access to the SCA's broad jurisdictional provision, the need to establish probable cause as to the jurisdictional location of the suspect's cell phone when the warrant is obtained would prevent law enforcement from locating violent and presently dangerous criminals such as the one in this example. Motion Hearing Recording at 2:12:20 (September 6, 2024).

The Court is not convinced. If the suspect had just robbed a bank in Mississippi and there was no information that he had traveled elsewhere, these facts support a finding of probable cause that his phone remained in Mississippi. "[P]robable cause is a matter of probabilities and common sense conclusions, not certainties." *United States v. Biglow*, 562 F.3d 1272, 1280 (10th Cir. 2009) (internal quotation marks omitted). The fact that the suspect turned out to have traveled elsewhere would not invalidate the probable cause determination, which was based on information known at the time the warrant was issued.

Granted, in rare instances, the government might know that a suspect has left one state but have no idea to what other state the suspect traveled. In such an instance, however, instead of obtaining a § 2703(c)(1)(A) ping warrant, the United States could obtain a § 2703(c)(1)(A) warrant (or even § 2703(d) warrant) for a record of the suspect's location on the day the warrant is signed (or on some future date through an anticipatory warrant). Once the United States receives this information, armed with fresh probable cause of the suspect's location, the United States could then obtain its tracking warrant.

At the September 6 hearing, the United States also claimed that obtaining a one-time disclosure of the suspect's location would take too long—at least two weeks. Motion Hearing

[20] The suspect turned out to be in Oklahoma—a fact that aided in the investigation of the suspect, who was ultimately killed in a shootout in Arizona. *Id*.

Recording at 2:14:03 (September 6, 2024). Presumably, however, if getting a record of a suspect's location at one point in time would take two weeks, getting a ping warrant (multiple records of a suspect's location at multiple points in time) would also take two weeks, if not more. And, even if it turns out that getting numerous records for numerous time periods is quicker than getting one record for one point in time, this anomaly is no reason to alter the plain meaning of a statute.

b. Requiring the United States to notify a suspect after tracking has ended or else obtain an order delaying such notification is precisely what the Rules of Criminal Procedure contemplate when law enforcement tracks a person's location for an extended period.

In addition to arguing against application of the TDS's jurisdictional provision, the United States argues that ping warrants should not implicate notification provisions that apply to tracking device warrants. Specifically, Rule 41 contains the following notification provision that applies to tracking device warrants: "Within 10 days after the use of the tracking device has ended, the officer executing a tracking-device warrant must serve a copy of the warrant on the person who was tracked or whose property was tracked." Fed. R. Crim. P. 41(f)(2)(C). Extending this requirement to the tracking of cell phones, argues the United States, would "not make sense" because officers "may not know the identity, much less the address, of the person who owns the device whose location data is being collected." Doc. 5 at 10. This argument is unconvincing.

First, based on the Court's review of more than 200 ping warrants, it is very rare that law enforcement does not know the identity of the person they are tracking. Second, in the case of a physical tracker attached to a vehicle, in which the United States acknowledges Rule 41's notice provision applies, agents similarly may not always know who owns the car or where that person lives. Yet, the United States does not argue the occasional difficulty in identifying the person it is tracking through a physically installed tracker should cause that tracking device to be defined as

something different. Third, if law enforcement has probable cause to track a person using a cell phone number, it also has grounds to obtain subscriber information related to that telephone number. Even if the subscriber and user of the phone are different people, notifying the subscriber of the phone would at least constitute an attempt to notify the person whose property was tracked. Fourth, compliance with Rule 41's notice provision does not require the United States to know the identity of the person tracked. Presumably, even if the United States did not know the identity of the person it had been tracking for a month, having tracked the person for a month, it should nonetheless be easy for the United States to find and notify the tracked person about the tracking. Fifth, even if extremely rare instances exist in which the United States could not locate and notify the person it had just been tracking for a month, this provides no reason to deviate from the plain meaning of § 3117(b). Sixth, the United States is unlikely to frequently notify a tracked suspect of the tracking within ten days after that tracking has ended. This is because the United States' investigation is rarely complete within ten days after its tracking of a suspect has ended and so notification of the suspect would "seriously jeopardiz[e] an investigation." 18 U.S.C. §§ 2705(a)(2)(E) and 2705(b)(5). For the vast majority of ping warrants, the ongoing nature of the investigation will allow the United States to obtain an order under 18 U.S.C. § 3103a that extends its deadline to notify the suspect being tracked of the tracking. *See* 18 U.S.C. § 3103a(b)(1) (cross-referencing adverse results listed in 18 U.S.C. § 2705).

Indeed, one of the United States' arguments against defining as tracking devices the cell phones used to track a suspect's location is that doing so would create a "flood of filings" under § 3103a. *Id.* at 10 n.8. However, that the United States must keep track of extensions and notification requirements is nothing new. When the United States obtains a ping warrant it

routinely also obtains a § 2705(b) order in which the court prohibits the cell phone company from notifying its customer about the government's tracking. These gag orders are not eternal. Section 2705(b) permits the United States to "apply to a court for an order commanding a provider . . . for such period as the court deems appropriate, not to notify any other person of the existence of the warrant . . . ." 18 U.S.C. § 2705(b). Typically, the United States requests, and the Court grants, orders of a year in duration. Thus, the United States must already keep track of orders similar to § 3103a delayed notice orders for almost every ping warrant it obtains.

The United States must also already keep track of many other types of orders. For instance, the United States obtains PRTT orders more often than ping warrants. And 18 U.S.C. § 3126 requires the Attorney General to provide an annual report that includes the period of interceptions authorized by the order; the number and duration of any extensions of the order; the offense specified in the order application or extension; the number of investigations involved; the number and nature of the facilities affected; the identity of the law enforcement agency making the application; and the person authorizing the order. Thus, administrative challenges from voluminous records and reporting requirements are not new for the United States. Whatever administrative burdens come with keeping track of when § 3103a extensions expire do not justify distorting the plain meaning of § 3117(b).

This is particularly true considering that the tracking done through ping warrants is more invasive than the tracking usually done after an agent's physical installation of a tracking device. *See Carpenter*, 585 U.S. at 311 ("historical cell-site records present even greater privacy concerns that the GPS monitoring of a vehicle we considered in *Jones*"; tracking a person through their cell phone records provides "near perfect surveillance" akin to an ankle monitor). That is, tracking of a person's vehicle is less intrusive than the tracking of a person's every

movement through the cell phone the person carries. *Id*. ("While individuals regularly leave their vehicles, they compulsively carry cell phones with them all the time. A cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales."). When the United States physically places a tracking device on a car, Rule 41's notice provisions indisputably apply and so the government must notify a suspect of the tracking within ten days or else obtain a notification extension. It would be incongruous for the less intrusive tracking of a person's vehicle to have greater notification requirements than the "near perfect surveillance" that comes with cell phone tracking.

The United States' final notice-related argument points out that the SCA contains a provision to order a phone company not to notify the suspect of the warrant. Doc. 5 at 10 (presumably referencing 18 U.S.C. § 2705). The United States asks, "if notice is due to the 'person who was tracked,' and can be delayed through 18 U.S.C. § 3103a(b), why did Congress create a separate mechanism to delay *providers* from notifying their subscribers?" *Id*. (emphasis in original) (quoting *In re Monitoring of Glob. Positioning Sys. Info.*, 646 F. Supp. 3d 116, 127 (D.D.C. 2022)). This question assumes a provision that allows the government to delay notice to the person being tracked is in conflict with a provision that prevents the cell phone company from also telling that person about the tracking.

These provisions are not in conflict. The Supreme Court, through its promulgation of Rule 41, apparently felt it important that law enforcement tell persons who they tracked of such tracking. *See* Fed. R. Crim. P. 41(f)(2)(C) (setting forth notice requirement). It also understood, however, that reasons may exist for delaying such notice. Thus, Rule 41(f)(2)(C) includes a delay provision. But allowing the government to delay notice to the person it tracked would serve no

purpose if that person's cell phone company notified its customer of the same tracking. If law enforcement's delayed notice to the suspect is to be effective, it was essential for Congress to also ensure that the government have a mechanism to prevent the suspect's cell phone company from providing the same notice. Thus, the Court views provisions allowing for delayed notice to a suspect as operating in harmony, not in conflict, with provisions that prohibit a cell phone company from providing the same notice.

Indeed, Rule 41's notice and delayed notice provisions (relating to government notification of the person tracked) are connected to § 2705 of the SCA's gag order provisions (preventing a cell phone company from notifying its customers that the government obtained their records). The connecting path starts with Rule 41(f)(2)(C). This rule requires notice within ten days after the use of the tracking device has ended, but also provides that "[u]pon request of the government, the judge may delay notice as provided in Rule 41(f)(3)." Rule 41(f)(3) allows a judge to "delay any notice required by this rule if the delay is authorized by statute." The statute that authorizes such delay is 18 U.S.C. § 3103a(b), which among other prerequisites, allows for a delay where immediate notification "may have an adverse result (as defined in section 2705 . . .)." 18 U.S.C. § 3103a(b)(2). Sections 2705(a)(2)(E) and 2705(b)(5) of the SCA define an adverse result to include "seriously jeopardizing an investigation . . . ." Accordingly, Rule 41's reliance on § 2705 demonstrates that these provisions are intended to work together and are not in conflict.

In sum, the notification and delayed notification provisions contained in the SCA and Rule 41 provide no reason to alter § 3117(b)'s definition of a tracking device.

E. The relevant question is whether a device functions to track a suspect's movements, not whether agents need to install a device.

At its core, the problem with the United States' result-driven argument is one common to most result-driven arguments. Arriving at a result by focusing only on the desired final destination, rather than using fundamental principles as a guide to a final destination, places the United States on a wandering path ill-equipped to address unanticipated situations. Reduced to its essence, the United States' argument is that whether an electronic device constitutes a tracking device should turn on whether that device is installed, not on whether that device tracks a person's movement. The Court disagrees—what function a device performs is perhaps the most important consideration in defining that device. In contrast, whether a device is installed has little bearing on the definition of the device.

The Supreme Court's decision in *United States v. Jones*, 565 U.S. 400 (2012), provides a good starting point for the foundational principles that should govern the issue before the Court. There, the United States obtained a warrant authorizing the installation of a tracking device in the District of Columbia within ten days. *Id*. at 402-03. On the eleventh day, in the District of Maryland, agents installed the tracking device on the suspect's Jeep. *Id*. at 403. In opposing a motion to suppress evidence obtained from this tracker, the United States did not argue that its warrant was valid. *Id*. Instead, it contended, and the district court agreed, that a defendant has no reasonable expectation of privacy in his movements from one place to another on public thoroughfares. *Id*. Therefore, the district court denied the defendant's motion to dismiss evidence of his travel on public thoroughfares. *Id*.

The Supreme Court agreed that a person's reasonable expectation of privacy is a relevant consideration. *Id*. at 406-11. But, the Supreme Court held, it is not the only consideration. *Id*. In deciding whether a Fourth Amendment violation occurred, the Supreme Court explained it first

looks to whether the agent's installation of the tracking device constitutes a trespass. *Id*. If the answer to this question is "yes," a Fourth Amendment violation occurs, suppression of the location information is necessary, and consideration of whether the government also violated the suspect's reasonable expectation of privacy is unnecessary. *Id*. Because the agents in *Jones* installed the tracking device without a valid warrant, the Supreme Court held that use of the tracking device violated the Fourth Amendment. *Id*. at 411-12.

Thus, *Jones*' extensive discussion about the installation of a tracking device makes clear that installation is relevant to jurisdiction and trespass. As § 3117(a) and *Jones* make clear, if installation does not occur in the same district where the tracking warrant is obtained, the tracking warrant is invalid. If agents install a tracking device without a warrant, they commit a trespass that requires suppress of evidence obtained from the tracker. With all of *Jones*' discussion about the significance of installation, however, the Supreme Court provided no indication that the character of the device at issue might turn on whether that device was installed. In fact, the opposite is true.

In 2012, when the Supreme Court decided *Jones*, the smartphone market was already in full force. Although *Jones* itself did not concern smartphones, it did acknowledge that it might eventually have to address "cases that do not involve physical contact, such as those that involve the transmission of electronic signals."[21] *Id*. at 411. As long as these cases do not involve a

[21] Although the majority opinion stopped short of saying, "such as cell phones," the majority was responding to arguments the concurrence made. *Id*. at 411 ("The concurrence faults our approach for 'presenting particularly vexing problems'. . . ."). In her concurrence, Justice Sotomayor noted, "With increasing regularity, the government will be capable of duplicating the monitoring undertaken in this case by enlisting factory- or owner-installed vehicle tracking devices or GPS-enabled smartphones." *Id*. at 415. Similarly, Justice Alito in his concurrence wrote, "Perhaps most significant, cell phones and other wireless devices now permit wireless carriers to track and record the location of users . . . ." *Id*. at 429. Thus, it is fair to say that cell phones were among the non-agent-installed devices the majority had in mind.

trespass,[22] the Court indicated the need for a warrant will turn on the tracked suspect's reasonable expectation of privacy. *Id*. at 412-13. And the Supreme Court explicitly declined to decide whether warrantless prospective location monitoring through signals sent from a suspect's phone would violate the Fourth Amendment. *Id*. at 412 ("It may be that achieving the same result [of visual surveillance] through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy, but the present case does not require us to answer that question . . . . We may have to grapple with these 'vexing problems' in some future case where a classic trespassory search is not involved and resort must be had to *Katz* analysis; but there is no reason for rushing forward to resolve them here.").[23]

More important for the present analysis, however, is that nothing in *Jones* indicates that the nature of the device used to track a person's location turns on whether an agent must install the device. Installation is relevant to trespass considerations but has no bearing on a person's legitimate expectation of privacy recognized in *Carpenter*—"privacy in the record of his

[22] Justice Sotomayor's concurrence demonstrates that deciding whether a device has been installed, which relates to the question of trespass, is not as straightforward as the United States posits. She notes that deciding whether an installation has occurred "in cases involving surveillance that is carried out by making electronic, as opposed to physical, contact with the item to be tracked" will "present particularly vexing problems." *Id.* at 426. As an example, she asks, "[S]uppose that the officers in the present case had followed respondent by surreptitiously activating a stolen vehicle detection system that came with the car when it was purchased. Would the sending of a radio signal to activate this system constitute a trespass to chattels? Trespass to chattels has traditionally required a physical touching of the property." *Id.* Thus, installation is not as simple a litmus test for whether something is a tracking device as the United States makes it seem. *See also* Steven Wm. Smith, *The Cell Phone Donut Hole in the Tracking Device Statute*, 14 Fed. Cts. L. Rev. 1, 23-26, 31, 35-36 (2021) (asserting that software installation, as opposed to a physical installation on the thing being tracked, qualifies as an installation for purposes of § 3117(a)).

[23] That the Supreme Court demurred on this issue is not relevant to the present analysis as cell phone location monitoring done through a ping warrant obviously does not implicate concerns associated with a warrantless search.

physical movements as captured through CSLI." 585 U.S. at 310. That is, installation has no bearing on what is at issue in the present case: Fourth Amendment foundational principles that apply when law enforcement uses a person's cell phone to track that person's movement for an extended period.

Further, language in *Carpenter* indicates that the Supreme Court would conclude that, when law enforcement uses a cell phone to track a person's movement, that cell phone functions as a tracking device. *Carpenter* explicitly states, for instance, that CSLI tracking is "[m]uch like GPS tracking of a vehicle . . ." *Id*. at 309. *Carpenter* also compares a cell phone's "near perfect surveillance" to another device that would indisputably meet the definition of a tracking device—an ankle monitor. *Id.* at 309, 312. Further, *Carpenter* notes that, "Apart from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data." *Id*. at 315. The Supreme Court's comparison of cell phone CSLI tracking to other devices that, even under the United States' definition, qualify as tracking devices, indicates that the Supreme Court would consider a cell phone to be a tracking device when used to track a suspect's location.

In *Carpenter*, the Supreme Court focused on what a cell phone does—it acts as a tracking device when law enforcement obtains CSLI for an extended period. In deciding whether a cell phone meets the definition of a tracking device in the present case, the Court also focuses on the function of the cell phone in providing law enforcement with location information. In contrast, the United States' result-driven focus on installation leads to illogical distinctions between different types of devices that might be used for tracking.

Recall the hypothetical agent who wedges his cell phone between the back seat cushions of a suspect's car during a controlled buy. Under the government's theory, this phone clearly

functions as a tracking device. It is an electronic device, an agent installed it, and it is being used to track the movement of the suspect or the suspect's property. Now consider a theft-protection electronic device a car manufacturer (not an agent) installs to provide a signal to locate a car when it is stolen. That device is not much different than the cell phone wedged between the back seat cushions, the tracking device agents installed underneath the vehicle, or the suspect's cell phone sitting next him as he drives down the road. What reason is there for applying different jurisdictional provisions, disclosure statutes, and procedural rules to these various methods of tracking? There is no principled reason. True, a result-driven reason exists. But the desire for a particular result does not justify deviation from principle.

The United States has provided no reason why a suspect should receive greater procedural protections under Rule 41 when tracked via a planted government phone than when tracked via government intrusion into the person's own phone. Indeed, the Supreme Court noted, "While individuals regularly leave their vehicles, they compulsively carry cell phones with them all the time. A cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales . . . ." *Carpenter*, 585 U.S. at 311-12. Thus, it concluded "historical cell-site records present even greater privacy concerns than the GPS monitoring of a vehicle we considered in *Jones* . . . ." *Id*. For the same reasons the Supreme Court articulated in *Carpenter*, prospective CSLI also presents even greater privacy concerns than the GPS monitoring of a tracker the United States installs on a suspect's vehicle. Consequently, to the extent that different procedural protections should apply to cell phone tracking than to a tracker physically installed on a suspect's vehicle, more, rather than less, protection should be provided to the cell phone tracking.

More important than even the degree of intrusion various modes of tracking cause, however, is that their essential function is all the same. The electronic device installed under the car, wedged between the cushions by an agent, pre-installed by the car manufacturer as a theft protection mechanism, or purchased by the suspect and sitting in his cup holder are all being used to track a person's movements over an extended period. In each instance, the person being tracked has a similar Fourth Amendment reasonable expectation of privacy. No principled reason exists to distort the text of the TDS and Rule 41 so that legal protections for individuals subject to tracking apply only when the government installs the device, as opposed to when the government avails itself of the technology a third party put in place.

F. Even accepting the United States' argument that a device cannot be considered a tracking device unless there is an installation, the United States' applications and proposed orders, on their face, call for an installation.

Lastly, and perhaps most importantly, even accepting the United States' argument that an electronic device used to track a person's movement cannot be considered a tracking device without an installation, the United States' warrant application, proposed order, PRTT application, and proposed PRTT order all call for an installation. Therefore, the cell phone at issue in the present ping warrant, even under the government's definition, would have to be considered a tracking device.

Specifically, the United States' warrant application requests an order "that authorizes the installation and use of a pen register and a trap and trace device," and its proposed order uses the same language. Doc. 8 at 21 (PRTT Application); Doc. 9 (PRTT Proposed Order). Thus, even accepting the United States' argument that an installation is a prerequisite to categorizing an electronic device as a tracking device, the United States' application requests an order for an

installation, its proposed order requires an installation, and the cell phone, therefore, meets even the government's definition of a tracking device.

G. Summary of reasons why the cell phone presently at issue constitutes a tracking device.

The plain text of 18 U.S.C. § 3117(b) clearly encompasses a cell phone and, given this unambiguous definition, no reason exists to look to the jurisdictional provision in § 3117(a) for clarification of this definition. No absurd result follows from this interpretation. And any added burden on law enforcement that derives from needing to delay notification under § 3103a is simply the cost Congress has determined appropriate to protect individual liberties. Such inconvenience does not justify an alternative interpretation of plain statutory language. The function of cell phone used to track a person's location is not meaningfully different from a tracker installed under a person's car, and there is no rational basis for treating them differently under the Fourth Amendment and accompanying legal provisions. And, even if categorization as a tracking device turns on whether there is an installation, the warrant the United States presently seeks calls for an installation. Consequently, a cell phone used to track a person's location on a real-time, rolling basis is a tracking device under the TDS, and a warrant to obtain that tracking information requires compliance with the Rule 41's tracking provisions.

V. Jurisdiction depends on an "installation" in the District of New Mexico.

Given the multitude of statutes, rules, and jurisdictional provisions at play, and to provide the United States guidance for future warrants, the Court now summarizes its jurisdictional analysis. The starting point is the Court's determination that, to justify a ping warrant, the Pen/Trap Statute and the SCA must combine forces.

Next, consider the TDS. Its jurisdictional provision, § 3117(a), states, "If a court is empowered to issue a warrant or other order for the installation of a mobile tracking device, such

order may authorize the use of that device within the jurisdiction of the court, and outside that jurisdiction if the device is installed in that jurisdiction." Note that Congress chose conditional words when it wrote this section. The use of *if* and *may* in this section make clear that this section does not apply in all circumstances. That is, if a device is not installed, its designation as a tracking device does not implicate § 3117(a).

However, the United States' ping warrant application, which depends in part on the Pen/Trap Statute, explicitly calls for an installation. *See* 18 U.S.C. § 3123(a)(1) ("Upon an application made under section 3122(a)(1), the court shall enter an ex parte order authorizing the installation and use of a pen register or trap and trace device anywhere within the United States . . . ."); Doc. 8 at 21 (PRTT Application) ("The United States of America . . . respectfully submits under seal this *ex parte* application for an order . . . that authorizes the installation and use of a pen register and a trap and trace device . . . ."). Because the cell phone described in the United States' warrant request is a tracking device and because, according to the United States' submission, an installation is necessary for the cell phone to function as a tracking device, the jurisdictional provision of the TDS, which governs where an installation must occur, is implicated.

This leads to the next question: When a device is not being physically installed, where does the installation take place? The United States' brief did not address where the installation to which it refers will occur. The location data at issue might be stored in a cell phone company's server that is located outside the District of New Mexico. Nonetheless, it is the suspect's cell phone that functions as the tracking device. If the cell phone's use as a tracking device occurs through some installation that happens while the cell phone is in the District of New Mexico, the Court will consider the installation to have occurred in the District of New Mexico. Thus, when

the United States seeks a tracking warrant for CSLI, as long as probable cause exists that the phone is located within the District of New Mexico when the tracking begins, the Court has jurisdiction under § 3117(a).[24] *Cf.* Stephen Wm. Smith, *The Cell Phone Donut Hole in the Tracking Device Statute*, 14 Fed. Cts. L. Rev. 1, 225 (2021) (discussing complications of remote installation); *United States v. Taylor*, 935 F.3d 1279, 1286 n.9 (2019) (government-installed malware that gathered suspects' computer data was sent from the Eastern District of Virginia but "installed" where the suspects' computers were located, causing jurisdictional problems).

In sum, the TDS's jurisdictional provision applies to cell phones used as tracking devices to obtain prospective location information under the hybrid authority of the Pen/Trap Statute and the SCA. This means that warrant applications must either demonstrate probable cause that the phone will be located in the District of New Mexico at the time the "installation" occurs (tracking begins) or that some other installation that renders the cell phone a tracking device will occur in New Mexico.

VI. Conclusion and next steps.

The Court finds that the SCA is insufficient, on its own, to allow for prospective, rolling production of cell phone location records at all times day or night. However, the SCA can operate in conjunction with the Pen/Trap Statute to establish this authority. If these statutes operate in conjunction, the cell phone for which records are obtained becomes a tracking device

[24] As noted in footnote 16, the United States' September 6 argument proceeded on the assumption that, if the TDS applies, the United States will have to demonstrate that the cell phone is in the District of New Mexico at the time tracking begins. In future warrant submissions, if the United States believes that some other type of installation has occurred in the District of New Mexico that meets § 3117(a)'s jurisdictional requirement, it may present such argument at that time. Similarly, if the United States in future warrant submissions would like to argue that the SCA's jurisdictional provisions trumps the TDS's jurisdictional provision, it may do so.

subject to the notice provision in Rule 41 and the notice-extension provision in 18 U.S.C. § 3103a. Because a cell phone becomes a tracking device and the Pen/Trap Statute requires an installation, the jurisdictional provision of the TDS applies and the government will need to establish probable cause that the phone will be in the District of New Mexico when the installation occurs (i.e., when tracking begins).

Warrants requesting location records over a fourteen-day period but *not* requiring the phone companies to provide the records on a rolling basis will not be considered tracking warrants and need only comply with the requirements of the SCA, not the hybrid approach described above. In other words, because the phone will not operate as a tracking device under these circumstances, Rule 41 procedures for tracking devices will not apply.

Going forward, for warrants submitted to the undersigned, the Clerk's Office will also conduct an initial screening to ensure that the warrants the United States submits do not contain administrative errors. For warrants seeking to track a person's movement in real time through the cell phone that person carries (similar to the ping warrant at issue here), agents should use Form AO 102. If agents seek electronic approval (as opposed to submitting the warrant application in person), agents should cross out the "Sworn to before me and signed in my presence" language contained on the bottom of the form and write in that the application is telephonically sworn and submitted by email. Similarly, if not submitted in person, the signature page of the agent's affidavit should indicate that the affidavit is being telephonically sworn and submitted by email. For the warrant, agents should submit Form AO 104. Warrant applications must not include a request to compel phone providers to "initiate a signal" as the United States has represented that when such a request is submitted, it is submitted in error. The Clerk's Office will summarily

reject tracking warrant applications submitted to the undersigned that do not comply with these procedures.

For the reasons contained in this Memorandum Opinion and Order, the Court rejects the United States' August 15, 2024, application for a warrant for location information (ping warrant).

IT IS SO ORDERED.

UNITED STATES MAGISTRATE JUDGE
STEVEN C. YARBROUGH